REMARKS

The above amendment and these remarks are responsive to the FINAL Office Action of Examiner Daniel J. Ryman, dated 5 Aug 2005.

Claims 1, 3-14, and 16-22 are in the case, none as yet allowed.

Specification

The disclosure has been objected to because of certain informalities, which applicants have corrected by this amendment.

35 U.S.C. 103

Claims 1, 3-14, and 16-22 have been rejected under 35 U.S.C. 102(b) over Srisuresh (P. Srisuresh, "RFC 2709 - Secuirty Model with Tunnel-mode IPsec for NAT Domains". Network Working Group, RFC 2709, October 1999. 1-9) in view of Applicant's Admitted Prior Art (AAPA).

Applicants traverse.

The Examiner refers to the Background section of

applicants' disclosure (AAPA) for the following teachings:

> "...both an outer connection and an inner connection be IP security connections in order to permit a remote user to connect to an enterprise using a VPN (page 2, line 7-page 4, line 14). [Office Action, page 3, 4, 6, 8.]

Applicants Background Art section to which the Examiner refers does not suggest that the art teaches coincident endpoints on one end, nor VPN NAT. As will be discussed below, that concept is also not taught by Srisuresh. (The Examiner includes page 4, lines 11-14 in the recitation of AAPA. However, this is a reference to a copending, commonly assigned application incorporated by reference into the present specification. It therefore is not properly considered as included in the AAPA.)

With respect to Srisuresh, the Examiner appears to have missed the point that the present invention is about nested connections with coincident endpoints on one end. That is not taught by Srisuresh, nor by AAPA.

Further, with respect to Srisuresh, the Examiner is apparently reading Srisuresh's "Tunnel mode IPsec" as referring to the same thing as nested IPsec connections. It does not. Tunnel mode IPsec does not refer to nested IPsec connections. As explained and shown in applicants' response to the previous Office Action as "Attachment", tunnel mode

IPsec is a kind of mode used by AH or ESP (the two IPsec protocols). The other is transport mode. Neither are about nested IPsec connections.

The present invention handles both tunnel and transport mode IPsec connections in any combination with outer and inner IPsec nested connections, in any combination of AH and ESP. In contrast, Srisuresh, only concerns tunnel mode IPsec connections, and non-nested ones at that. (This will be elaborated further, below.)

The AAPA does not teach nesting VPN connections with coincident endpoints on one end (nor VPN NAT).

Consequently, combining Srisuresh and AAPA does not result in coincident endpoints, and does not result in VPN NAT, and does not result in VPN NAT with coincident endpoints. It is this last combination which is the point of the present invention.

Regarding claims 1 and 10, Srisuresh does not disclose certain claimed aspects of the current invention.

First, Srisuresh does not use, mention, or disclose "an outer connection and an inner connection", by which it is clear in the current invention is meant two IPsec connections, one nested inside the other (see Fig. 2 and explanatory text at Page 10, lines 17-20). Srisuresh does mention tunnel mode IPsec, which is not the same as two

nested IPsec connections (please refer to summary information below on IPsec). In the current invention the two IPsec connections may independently be IPsec in transport mode or tunnel mode, and this is completely independent of the fact that they have a nested relationship. Hence, in the current invention all possible combinations are supported; transport mode inside tunnel mode, transport mode inside transport mode, tunnel mode inside tunnel mode and tunnel mode inside transport mode.

Srisuresh does mention an IP-IP tunnel (section 2.2), but this is not an IPsec connection. Hence any traffic inside this IP-IP tunnel is not inside an 'outer connection'. Srisuresh does mention that the IP-IP tunnel may contain IPsec traffic (an IPsec connection), but this is not what is claimed in the current invention, in claim 1, lines 1-5.

The Examiner recognizes that "Srisuresh does not expressly disclose that the outer connection and the inner connection are both IP security connections..." [Office Action, page 3.], but references AAPA for that teaching. However, all of applicants' claims reference "coincident endpoint" on the inner and outer connection, and that is not taught or suggested by either Srisuresh nor AAPA.

Thus, neither AAPA nor Sirsuresh teach two IPsec connections with coincident endpoints, as claimed. Sirsuresth have his IPC-NAT as the NAT node at apparently an

endpoint of his IP-IP tunnel (2.2). But, of course, this is not the same as two IPsec connections with coincident endpoints, nor is it the same as two IPsec connections one nested inside the other, with coincident endpoints at 'a first node'.

Sirsuresh's IPC-NAT and the current invention's VPN NAT (source-in) are both coincident with an endpoint of an IPsec tunnel, but this is not what the current invention claims. Hence, on this point, Sirsuresh in combination with AAPA does not teach the current invention.

To appreciate the next claimed difference between Sirsuresh and the AAPA, and the current invention, note that Sirsuresh repeatedly focuses the RFC and descriptions on 'tunnel mode IPsec' ("...capable of offering tunnel-mode IPsec security..." p1 abstract; "... can benefit from IPsec tunnel-mode security, when the NAT device acts as the IPsec tunnel end point." p2 2nd paragraph; "For purposes of this document, we will assume IPsec security to means tunnel mode IPsec security..." p3 1st paragraph of section 3; <and others>).

The current invention, throughout the text simply refers to IPsec connections, making no distinction to whether or not any of the IPsec connections are tunnel mode or transport mode. This is because the current invention applies to both modes of IPsec connections. And while Sirsuresh does not seem to explicitly rule out transport

mode IPsec, he does so in effect. Hence, on this point Sirsuresh in combination with AAPA does not teach nor suggest the current invention.

Further with respect to claims 1 and 10, each of which recites "performing source-in network address translation", Srisuresh and the AAPA distinguish the present invention on the details of the NAT performed on the decapsulated inbound packet. In Srisuresh, Fig. 4, IPC-NAT is shown to follow 'detunnel'. While Srisuresh does not mention source-in NAT (which is translation of the source IP address in the inbound packet), it does appear possible that this is allowed, when Srisuresh says "Any and all flavors of NAT mapping may be used..." [page 4, middle of second paragraph from bottom). However, there is more to the current invention in source-in NAT, as shown in Figure 4 and accompanying text. Neither AAPA nor Srisuresh include or mention the implicit MAP rule, the existence of an IP address pool for source-in NAT, how the IP address pool is configured or defined, nor how the implicit MAP rule is generated based on the IKE IDci and the IP address pool.

Concerning the last clause of claim 1; some elements of Srisuresh and the current invention are similar, but even so, applicants argue, Srisuresh with AAPA does not teach the claim. Similar elements are that NAT (some kind) is performed on the outbound packet, and the NAT is done on the same node as the endpoint of an IPsec tunnel. However, in Applicants' claims, since two IPsec connections are being

used, one nested inside the other with a common endpoint, the source-in NAT associated with the inner IPsec connection must be done prior to its encapsulation in both IPsec connections; this is not taught by Sirsuresh (which does not use nested IPsec connections) nor the AAPA.

Regarding claim 3 -- claim 3 deals with particulars of setting up the two, nested IPsec connections as shown in Fig 2 of the current invention, such that they work. That is, in such a manner that source-in VPN NAT can be configured for the outer T1 52 IPsec connection, and this will automatically and correctly be applied to the later established inner T2 54 IPsec connection. Since Sirsuresh and the AAPA do not deal with nested IPsec connections with a coincident endpoint, they clearly do not teach claim 3 in general. And less so in any of the following particulars.

First, more specifically, Sirsuresh does not configure an outer IPsec connection as the Examiner states (Office Action, page 4); how could it since it does not deal with nested IPsec connections with a coincident endpoint.

Second, Sirsuresh does not teach "communicating from a client to a gateway on said outer connection a request to configure a secure inner connection". Sirsuresh does not do this at pages 5-6, section 4 or Fig 5, to which the Examiner refers.

Third, Sirsuresh states, again (Page 5, 1st paragraph

of section 4), "In other words, we will focus on the operation of IKE in conjunction with tunnel mode IPsec...". The current invention works for all IPsec modes, not just tunnel mode, and for both AH and ESP protocols, and all combinations thereof.

Fourth, with respect to the 3rd clause of claim 3, Sirsuresh does teach this; "IKE will communicate the negotiated security parameters directly to the IPC-NAT gateway engine as described in the following diagram.", referring to Sirsuresh Fig. 5. This is an aspect of similarity between Sirsuresh and current invention; both involve communicating something from IKE to something related to NAT. Sirsuresh uses 'policies', and the current invention uses IPsec Security Associations. However, since Sirsuresh does not deal with nested IPsec connections having a coincident endpoint, he does not anticipate "initializing said gateway to receive a future nested communication". This initialization contains the specifics for source-in NAT, the use of the address pool, generating the implicit MAP rule and loading the VPN NAT implicit MAP rule. None of these technical specifics is taught by Sirsuresh nor the AAPA.

Fifth, Sirsuresh does not teach 'starting said inner connection'.

Sixth, Sirsuresh does not teach the last clause of claim 3; "responsive to starting said inner connection,

propagating a network address translation rule from said outer connection to said inner connection". This step relates to functioning and automatic setup of nested IPsec connections with VPN NAT and a coincident endpoint, because (as will be appreciated in Fig. 2), subsequent outbound packets destined for the remote node that initiated the inner connection must have VPN NAT (source-in NAT as in Fig. 4) applied to the outbound destination IP address before the packet is encapsulated inside the inner IPsec connection, and appropriate to the mode of that connection. This propagation of the VPN NAT rule specific for a given inner IPsec connection is necessary because there may be multiple inner connections from multiple remote nodes, and each must have its own unique IP address on the internal side of the 'first node' (50 in Fig 2). This is not taught by the combination of Sirsuresh and AAPA.

Regarding claim 4, which depends from claim 3, Sirsuresh does not contain an inner IPsec connection. Sirsuresh and AAPA also do not contain an outer IPsec connection with coincident endpoint, nor does Sirsuresh or AAPA encapsulate a packet in the inner connection and then in the outer connection.

Regarding claim 5, which depends from claims 3 and 4, discussed above, Sirsuresh does not save any address translation rule included within said packet, as claimed. Hence Sirsuresh and AAPA do not teach claim 5.

Regarding claim 6, which depends from claims 3, 4 and 5, discussed above, Sirsuresh and AAPA do not contain nested IPsec connections with coincident endpoints, of any depth. Hence Sirsuresh and AAPA do not teach "iteratively executing said decapsulating step". Hence Sirsuresh does not anticipate claim 6.

Regarding claims 11 & 16, both claims recite "support for nested connections with coincident endpoints...". As discussed above with respect to claims 1, 3 and 10, Sirsuresh does not deal with nested IPsec connections nor with nested IPsec connection with coincident endpoints. Further, that claims 11 & 16 recite "... without requiring any special configuration for the inner connection...". Sirsuresh does not address how to do this.

As set forth specifically or by implication in various claims, several aspects solved in the current invention that Sirsuresh does not address, nor mention, include automatic initialization of inner IPsec connection VPN NAT rule for an outer IPsec connection, the automatic generation of the implicit VPN NAT rule (implicit MAP), the automatic IP address pool selection for the VPN NAT rule, the automatic loading of the VPN NAT rule on the outer connection, the later automatic propagation of the VPN NAT rule to the newly created inner IPsec connection, the application of the VPN NAT rule to outbound traffic to be doubly encapsulated in the two IPsec connections with a coincident endpoint, and all this support for multiple levels of nested connections,

and for multiple inner connections within a single outer connection. Applicants argue that these solutions are not taught and cannot be implied from the teachings of Sirsuresh and the AAPA.

With respect to claim 12, which depends from claim 11, Sirsuresh and AAPA do not teach or suggest starting an inner IPsec connection because there is no outer connection with a coincident endpoint.

With respect to claim 13, which depends from claims 11 and 12, Sirsuresh and AAPA neither teach nor suggest anything like "saving any VPN NAT rule included within said packet". And then, "applying said NAT rule...".

With respect to claim 14, which depends from claims 11-13, Sirsuresh and AAPA do not suggest the "iteratively executing said decapsulating step...". Sirsuresh' figures contain no loops, nor does the specification suggestion that looping might be necessary. Sirsuresh text does not contain a single mention of nested IPsec connections with coincident endpoints, nor of arbitrarily nested IPsec connections, which would be somewhat surprising since the whole focus of Sirsuresh is "...Tunnel-mode IPsec for NAT Domains" (title of the document). Again, note the 'tunnel-mode' as used in the title refers to IPsec tunnel mode (again, see IP Security Basics, below), and not to nesting of IPsec connections with coincident endpoints (which may be tunnel mode or not).

With respect to claims 17 & 18, which are related as the Examiner observes to the inventions set forth in claims 1 & 10, Applicants assert the same distinctions with respect to Sirsuresh and the AAPA as previously discussed with respect to claims 1 and 10. Applicants do not traverse the Examiner's assertion that it is well known in the art to implement certain computer methods with software. These claims are presented in support of licensing considerations, and the software aspects per se are not relied upon for distinguishing the art.

With respect to claims 19-22, these claims are structured similarly to claims 3-6, as the Examiner observes. Applicants refer the Examiner to the discussion above with respect to claims 3-6 for distinguishing Sirsuresh and AAPA. Again, these claims are presented in support of licensing considerations, and the software aspects per se are not relied upon for distinguishing the art.

Applicants urge that the rejection of claims 1, 3-14, and 16-22 be reconsidered and withdrawn.

SUMMARY AND CONCLUSION

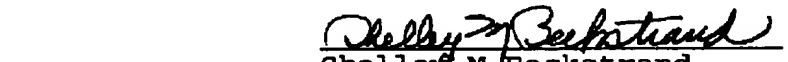
Applicants urge that the above amendments be entered and the case passed to issue with claims 1, 3-14, and 16-22.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. BODEN, ET AL.

By



Shelley M Beckstrand
Reg. No. 24,886

Date: 3 Oct 2005

Shelley M Beckstrand, P.C.
Patent Attorney
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: (276) 238-1972
Fax: (276) 238-1545